The Report Committee for Alicia Louise Leonard Moore
Certifies that this is the approved version of the following report:

Important Systems Engineering Analysis Tools: Failure Mode and Effects Analysis and Hazard Analysis

APPROVED BY
SUPERVISING COMMITTEE:

Anthony Ambler, Supervisor

Robert McCann

Important Systems Engineering Analysis Tools: Failure Mode and Effects Analysis and Hazard Analysis

by

Alicia Louise Leonard Moore, B.S.E.E.

Report

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Master of Science in Engineering

The University of Texas at Austin

December 2010

Dedication

This report is dedicated to the memory of my Mother, Betty Leonard. She taught me that I could do whatever I put my mind to. I also dedicate this report to my “sister by choice” Suzanne Magargee Meche who never lets me forget who I am.

Acknowledgements

A few years ago, a program at NASA Johnson Space Center was considering changes to the Failure Modes and Effects Analysis (FMEA) requirements when several key people felt that the FMEA Analysis was redundant to Hazard Analysis. My experience with manned space programs taught me that both analysis techniques provided different and unique results for Safety and Mission Assurance (S&MA), Systems Engineering and Program/Project Management. This paper is the result of the work that I did gathering data to attempt to convince management that the two analysis techniques are different and yield important information for programs and projects and to create courses to teach S&MA engineers the intellectual processes of FMEA Analysis and Hazard Analysis. This paper has existed in my head for the last three years and it was time to put it on paper.

I want to express my gratitude to Kevin Berry for his support and patience as we debated the pure Safety and Reliability vs. the Systems Engineering vs. the Program/Project aspects of the analysis techniques. His knowledge and experience improved my mind on several occasions during our debates and allowed me to embrace failure modes as an initiating event for a mishap.

Many thanks also go to Pete Spidaliere for his views on how the two analysis techniques are used for unmanned spaceflight projects. His unique views on the analysis techniques encouraged me to defend their value and show

how the right analysis techniques can enhance a spacecraft's design and be value added to the overall systems engineering process.

A very special thanks goes to Phil Deans and Joe Levine. I met both gentlemen when I was a very young Reliability Engineer working for Boeing Aerospace Corporation on the Safety, Reliability and Quality Assurance (SR&QA) contract for NASA/Johnson Space Center. Both Phil and Joe had a hand in making me the engineer that I am today. Phil helped me learn the FMEA process during the post-Challenger Return to Flight activities and Joe helped me learn many things in the overall SR&QA world. They both retired from NASA and became consultants. I was lucky enough to work with them again at SAIC in the mid-2000s. We had many long conversations about how the new programs and projects did not embrace the FMEA and Hazard Analysis techniques to improve their products. I am grateful to them both for improving my mind over the years and for the history that they provided for this report.

Last but not least I want to thank my professors for this report, Dr. Anthony Ambler and Mr. Bruce McCann of the University of Texas for working with me to finalize my report and for their insights during my course of study.

December 2010

Abstract

Important Systems Engineering Analysis Tools: Failure Mode and Effects Analysis and Hazard Analysis

Alicia Louise Leonard Moore, MSE

The University of Texas at Austin, 2010

Supervisor: Anthony Ambler

Abstract: The goal of every program or project manager is to have a safe reliable product and to have an understanding of the residual risk of operating that product. Two very important systems engineering analysis tools to achieve those objectives are Hazard Analysis and Failure Modes and Effects Analysis. Sometimes seen strictly as Safety and Reliability tasks, these analyses are key to a successful program or project and require input from all stakeholders. When viewed in the Systems Engineering process, Safety and Reliability are truly specialty disciplines within Systems Engineering. Hazard Analysis is used to improve system safety while Failure Modes and Effects Analysis is used to identify ways to increase product reliability; both analyses are required to improve systems design and fully capture the risk for a system or program. Depending on how the analyses are scoped, there could be a perception of overlap and duplication of effort. This paper will present a systems engineering approach to show the need and benefits for performing both types of analyses. Both analysis processes are required to ensure that all possible hazardous conditions and failure modes have been identified and addressed to minimize overall risk to the program/project and to ensure a safe and reliable system.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

There are many books on systems engineering that describe the overall systems engineering process and several of these books mention Failure Modes and Effects Analysis (FMEA) as well as Hazard Analysis, sometimes referred to as Safety Analysis. These books generally point to the specialty engineering fields of reliability engineering and safety engineering as the "place to go" for how to perform these two analyses. I don't want to discount the contributions from the S&MA community; however, systems engineers need to be aware of these analysis processes and take advantage of them throughout the lifecycle of their system. Often based on their past experiences, some systems engineers and project managers may jump to the conclusion that the results of the two analysis techniques are redundant and think that they can save resources by eliminating one of the processes. Although there are some similarities in some of the terms and steps of the two analysis processes, they have different goals and yield different results. The goal of FMEA Analysis is to make the system reliable and the goal of Hazard Analysis is to make the system safe. Without considering both analysis techniques you could end up with a very reliable system that is unsafe or a very safe system that doesn't work.

Reliability, in a generic sense, can be defined as "the probability that a system or product will perform in a satisfactory manner for a given period of time

when used under specified operating conditions."[1] The field of reliability engineering seeks to:

- Apply engineering knowledge and special techniques to prevent or reduce the likelihood or frequency of failures;
- Identify and correct the causes of failures that do occur, despite the efforts to prevent them;
- Determine ways of coping with failures that do occur, if their causes have not been corrected;
- Apply methods for estimating the likely reliability of new designs, and for analyzing reliability data.[2]

MIL-STD-882D Standard Practice for System Safety defines safety as freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. System Safety Engineers employ specialized professional knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify and eliminate hazards, in order to reduce the associated mishap risk.[3]

The purpose of this report is to show the importance of both FMEA Analysis and Hazard Analysis and how in the overall safety and mission success

---

[1] Blanchard, Benjamin. *Systems Engineering Management.* 2nd. New York: Wiley, 1998. Print.

[2] O'Connor, Patrick D. T. *Practical Reliability Engineering.* 4th. West Sussex: Wiley, 2002. 2. Print.

[3] Department of Defense. *MIL-STD-882D Standard Practice for System Safety.* Washington: Department of Defense. 2000. 2. Web 4 November 2010.

of a project and to show how both analyses are required to improve systems design and fully capture the risk for a system or program. Depending on how the analyses are scoped, there could be a perception of overlap and duplication of effort. This paper will present a systems engineering approach show the need (and specific benefits) for performing both types of analyses. Both analysis processes are required to ensure that all possible hazardous conditions and failure modes have been identified and addressed to minimize overall risk to the program/project.

Chapter 2: Failure Modes and Effects Analysis

WHAT IS FMEA?

Many people use the term FMEA as a noun and as a verb. FMEA the verb is the structured bottoms up intellectual process to evaluate a system design for possible failure modes and causes early in the design process so that mitigation options can be developed to “deal with” the causes of the failure mode. FMEA the noun is generally the documentation that captures the results of the analysis. This section concentrates on FMEA the verb and will use the phrase FMEA Analysis to distinguish between the noun (the FMEA report) and the verb (the FMEA Analysis). The process for FMEA Analysis is formally documented for general use in *MIL-STD-1629A – Procedures for Performing a Failure Mode, Effects and Criticality Analysis (FMECA).* NASA calls the process FMEA/Critical Items List (CIL).

FMEA Analysis should be performed by a multi-discipline team early in the design phase to aid in the evaluation of the design. Used properly, FMEA Analysis will allow engineers to anticipate failure modes before they happen and to eliminate the failure mode with redesign or mitigate the effects of the failure by other means.

During the design and development phase, when design criteria, mission requirements, and conceptual designs are being developed, the results of the FMEA Analysis are used to evaluate the design approach and to compare the benefits of competing design configurations. FMEA Analysis provides a systematic identification of failure modes and their associated causes for evaluation, as well as identifying potentially critical single failure points for possible elimination or mitigation.

As the mission and design definitions become more refined, FMEA Analysis is expanded to successively more detailed levels. When changes are made in the design to remove or reduce the impact of identified failure modes, FMEA Analysis must be repeated for redesigned portions to ensure that all predictable failure modes in the new design are considered.

HISTORY OF FMEA AT NASA

The idea of FMEA was developed by the United States Military and documented in Military Procedure MIL-P-1629 “Procedures for Performing a Failure Mode, Effects and Criticality Analysis” dated November 9, 1949. The military used the analysis to evaluate the effect of system and equipment failures and then classified the failures according to their impact on mission success and safety. The Project Mercury and Gemini Programs had no reliability or quality assurance requirement documents that could be imposed contractually on the contractor. The Project Mercury and the Gemini Programs depended on their early spacecraft experience (e.g. X-Series aircraft programs) from National Committee for Aeronautics (NACA) and the contractor experience obtained from Department of Defense (DoD) aircraft and missile programs.[4] The requirements were formalized during the Apollo Program when an engineer named Joe Levine, with a background in military flight tests, was tasked to develop requirements for reliability, quality and test. North American Corporation had just been awarded the contract for the spacecraft and there were no reliability documents. It is important to note that safety analysis was not included at that time and it was only added after the Apollo 1 fire. Joe used MIL-R-27542 from the US Air Force,

[4] Levine, Joe, Marion Merrell and Jeff Adams. *JSC SR&QA Evolution Resulting from Manned Spacecraft Program History.* Working Paper. 2002. 5. Print.

which established the minimum essential contractor reliability effort to assure acceptable reliability in an Air Force system, as his starting point. He wanted to improve reliability through test and analysis to verify requirements. He also wanted to integrate quality and reliability into the overall systems engineering process. He started promoting the idea of performing FMEA Analysis by asking the engineers, "How do you know that your design will work without failure?" Although initially the value of this analysis was not recognized, Joe continued promoting the process and began to show the engineers how the results of the FMEA Analysis would improve their designs. Furthermore, he worked with the engineers to improve the test procedures to "test for" the failure modes that were identified. The concept of "show me that the failure won't occur" has grown into what is now known as retention rationale required for critical failure modes.[5] Each of the major manned space programs and the NASA field centers has established requirements and processes for application of the analysis to their products.

OBSTACLES IN THE FMEA PROCESS

Sometimes programs or projects do not see the value added in the FMEA process because the process has broken down. In order to provide value to the program or project, the FMEA process needs to start early in an organized fashion with management support. When discussing the value of FMEA with engineers from many different engineering disciplines, the responses ranged from "waste of time" and "I don't want to do anything with it" to "powerful tool, effective way to prevent problems" and "needs to be done across the board."

There are many obstacles in the process:

---

[5] Levine, Joe. Personal Interview. 19 November 2008.

- **Only one person assigned to do the analysis** – Sometimes a manager will assign a reliability engineer the task of doing FMEA for a system. This is ineffective as a team of one is seldom as successful as a team of the right people. All of the stakeholders need to be involved – this is NOT just a Safety and Mission Assurance (S&MA) exercise, you need diverse representatives from the project team including but not limited to Design Engineering, S&MA, and Operations.
- **Design or process expert is not included in the FMEA team or is allowed to dominate the team** – design engineering has to be included but cannot dominate the analysis process.
- **FMEA team does not have comprehensive knowledge of the system of interest** – The team MUST know the system of interest: its function, how it operates, what's in the systems and what's not in the system, its interfaces, etc.
- **FMEA team has not been properly trained** – "making it up as you go" is a recipe for disaster, the team must understand the intellectual analysis process as well as the program specific requirements governing classification of the analysis results.
- **FMEA team becomes bogged down in the minute details and loses sight of the overall objective** – the objective of the FMEA Analysis is to identify all credible failure modes with the goal of eliminating when possible and providing strong retention rationale when not possible
- **FMEA team rushes through the process to "get on with" the design and building** – FMEA takes a great deal of time to complete. It essentially the "pay me now or pay me later" concept. Time spent up front identifying ways to eliminate the failure modes or manage the

effects has a very high return on investment if you avoid catastrophic or critical events in the future. If the team rushes through the process they could miss significant but obscure failure modes.

- **Too general** – FMEA team lists the same failure condition for every failure mode or lists a failure mode that is too generic e.g. fails to function. If all of the results are the same then the product is meaningless.
- **FMEA is started late in the design process** – if the FMEA Analysis is started after it is too late affect the design early in the process, then the "pay me now or pay me later" concept applies.
- **Management does not allow enough time** – this could be because they do not understand what it takes to complete the process or they do not understand the value of the results or it could be that designing and building hardware seems more productive than analyzing hardware.

THE ANALYSIS PROCESS

Figure 1 illustrates the overall FMEA Process. It is important to note that the process is iterative once your system has been defined and the cycle will happen multiple times in the overall project life cycle. As the design becomes more mature, you'll revisit the analysis and make adjustments as required.

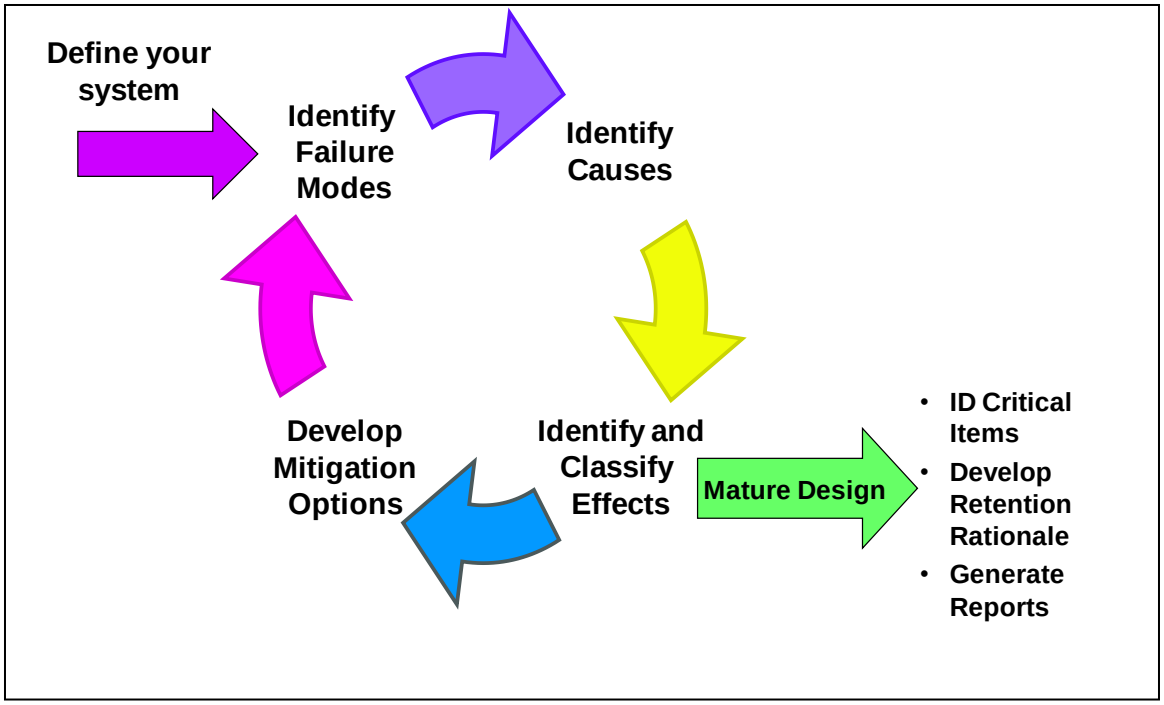

Figure 1 – The Overall FMEA Process

Define Your System of Interest

Before the analysis can begin, the analysis team must know what the system of interest is and how it works. The team must consider all of the elements listed below and ensure that the entire team has a common understanding.

- Description – use block diagrams and other models.
- Boundaries – where the system begins and ends is very important as you consider the effects of the failures.
- Interfaces – you need to know all of your interfaces to ensure that you understand how failures in your system could affect other systems.
- Functions – how your system works and what it is supposed to do.
- Ground Rules and Assumptions – document any assumptions and ground rules that the team has agreed to.

Identify Failure Modes

Once the team understands how the system should work, they need to identify ALL credible failure modes. As a starting point, the analysis team should consider the following basic failure conditions:

- Premature operation
- Failure to operate within specification or at a prescribed time
- Intermittent operation
- Failure during operation, including failure to contain or store energy or fluids
- Failure to cease operation at a prescribed time
- Degraded output or operational capability

There are other sources to assist in the identification of failure modes:

- Actual operational failure history of identical or similar items
- Actual developmental/testing failure history of the hardware or similar items
- Published sources of historical failure mode data
- Generic Failure modes
- Released and controlled component, assembly, detailed engineering drawings and specifications
- Training aids, such as cross-section drawings, photographs, and exploded assembly drawings
- Engineering knowledge.

Identify Causes

For each postulated failure mode, the analysis team must identify potential failure causes. Failure causes are the physical or chemical processes, design defects, quality defects, part misapplication, or other processes which are the basic reasons for failure or which initiate the physical process by which

deterioration proceeds to failure.[6] Good sources of failure causes are: heritage system failure history, generic failure causes, and engineering knowledge/experience and judgment. The major programs at the Johnson Space Center provided suggested failure causes in their program requirements and processes.

Develop Mitigation Options

Once all of the causes have been identified, the team needs to think about how to ensure that the system will work. The team needs to identify mitigation options to address each of the causes that were identified. The first goal should be to eliminate the cause. If the cause cannot be eliminated by design, the team should identify features of the design that will reduce the likelihood of the cause occurring through design features, manufacturing controls, process controls, tests, or inspections. Design features can be: material selection, parts derating, parts selection, or application of industry standards for strength, sizing, derating, etc. Some engineers will try to use redundancy as a mitigation option, but remember you are trying to eliminate or reduce the chances of the cause occurring and manifesting itself in a failure mode. While redundancy will eliminate single point failures, redundancy only addresses the effect of the failure mode occurring, so redundancy may not be a valid mitigation option to eliminate the cause, however, you may consider redundancy when addressing how to mitigate the effects of the failure mode. There are many standards that have been developed documenting “best practices” to assist in the process of mitigating causes.

---

[6] Department of Defense. *MIL-STD-1629A Procedures for Performing a Failure Mode and Effects and Criticality Analysis.* Washington: Department of Defense. 1980. 4. Web 4 November 2010.

Part two of this step is defining how to deal with the failure if it does occur. If, despite all of the great things that were done to reduce the likelihood of the causes; the failure occurs, what can be done? In other words, what actions are available to negate or mitigate the effect of a failure on a system, these actions are called compensating provisions.

- Define fault detection methods – becomes a design requirement – how can the failure be detected?
- Define fault isolation methods – may become a design requirement – how can the failure be isolated?
- Define fault recovery methods, including ground and/or crew actions – becomes an operational requirement – The team must identify compensating provisions (e.g. redundancies and other protective features that can regain the original function or protect from the effects of the failure.

Identify and Classify Effects

Identify the effects on all functions and operations. There are probably multiple effects including the worst case doomsday effect which is most likely different from the effect that has the highest probability of occurrence. The team must describe the credible failure effects at the following levels:

- Immediate Effect – the failure effect on the item under analysis, the assembly it is associated with (if appropriate), and its interfaces
- Next Effect – the failure effects at the next higher assembly level, typically the subsystem/system
- End Effect – The failure effects at the integrated vehicle level, including the effects on the mission and the crew

The team then estimates the time from failure occurrence to the manifestation of the worst case effect. The standard time categories are:

- Immediate – less than 1 second
- Seconds – 1 to 60 seconds
- Minutes – 60 seconds to 60 minutes
- Hours – 60 minutes to 24 hours
- Days – 24 hours to mission complete

In order to assist the program/project manager in understanding the severity of the failure modes, classify the effects of the failure modes. Typically each program or project will tailor the definitions of severity classification (e.g. criticality) to suit their individual needs but the standard categories from *MIL-STD-1629A Procedures for Performing a Failure Mode, Effects and Criticality Analysis* are:

- Category I – Catastrophic – A failure which may cause death or weapon system loss (i.e. aircraft, tank, missile, ship, etc.)
- Category II – Critical – A failure which may cause severe injury, major property damage, or major system damage which will result in mission loss.
- Category III – Marginal – A failure which may cause minor injury, minor property damage, or minor system damage which will result in delay or loss of availability or mission degradation.
- Category IV – Minor – A failure not serious enough to cause injury, property damage, or system damage, but will result in unscheduled maintenance or repair.[7]

[7] Department of Defense. *MIL-STD-1629A Procedures for Performing a Failure Mode and Effects and Criticality Analysis.* Washington: Department of Defense. 1980. 10. Web 4 November 2010.

Identify Critical Items and Develop Retention Rationale

Once the severity of each of the failure modes has been identified, the critical items can be identified. Each program or project will have their own definitions of critical items but they will typically include catastrophic and critical failure modes. Since it is highly improbable that you will be able to "design out" all of the catastrophic and critical failure modes, you will need to provide other options that can be accomplished to reduce the likelihood of the failure occurring or how you can reduce the effects of the failure. Again programs or projects will tailor what is required to document rationale for acceptance but the following categories are generally accepted and will be leveraged from your "recommended options" activities from the "Develop Mitigation Options" step in the process:

- Design – identify specific design features that will minimize the probability of occurrence of the failure mode. Examples include – increased factors of safety, material selection, addition of redundancy;
- Test – identify specific tests performed during manufacturing, hardware acceptance, system integration or ground processing that would detect the presence of the critical failure cause that would not be compromised by later processing activities. Examples include: test procedures, ground checkout, preflight checkout;
- Inspection - identify specific inspections performed during manufacturing, hardware acceptance, system integration or ground processing that would detect the presence of the critical failure cause that would not be compromised by later processing activities. Examples include: manufacturing inspections or ground turnaround inspections;

- Operational Use – describe the operational techniques that could be used to mitigate the effects of the failure once it has occurred such as operator actions to circumvent or mitigate the effect of the postulated failure;
- Failure History – Include all failure history for failure mode listed for this particular design or a similar design. This information ties the FMEA process to the problem reporting process in Quality Assurance – when failures occur, the retention rationale should be reviewed as part of the approval process to ensure that no failure modes or effects have been overlooked.

The retention rationale discussed above is important to the program or project so that they know that appropriate steps have been taken to minimize the risk of failures.

Generate Reports

This is the final step in the process and the format of the reports can be as simple as a spreadsheet documenting the analysis results to the volumes of information captured for manned space programs. Each program or project will set the requirements for the documentation required. It should be noted that the FMEA reports should be updated as new information is realized during the design process. Typical elements of FMEA reports are:

- Scope of analysis – what's in and what's out – the system definition;
- System description – to the level required for management to understand your results;
- Failure modes, causes, criticality assignment, retention rationale;
- Supporting data – "In God we trust, all others bring data";

- Executive summary – the bottom line for management – what's critical and why it is acceptable to fly with the potential failure modes?

The reports are very important first they serve as documentation for management of the residual risk for the program or project and second they are an important historical reference for knowledge capture for programs with long lifetimes or for future programs wanting to take advantage of successful designs.

BENEFITS OF FMEA

FMEA Analysis results in the identification of critical items and their associated rationale for decision making purposes. When done with discipline and rigor FMEA Analysis will:

- Improve the quality, reliability and safety of a product/process
- Improve company image and competitiveness
- Increase user satisfaction
- Reduce system development timing and cost
- Collect information to reduce future failures, capture engineering knowledge
- Reduce the potential for warranty concerns
- Allow for early identification and elimination of potential failure modes
- Emphasize problem prevention
- Minimize late changes and associated cost
- Serve as a catalyst for teamwork and idea exchange between functions

FMEA Analysis is a structured intellectual process that will identify all credible failure modes, eliminate failure modes by design (where possible), manage the remaining failure modes and their causes, and quantify risk based

on severity classification. FMEA Analysis is not an exact science it relies on engineering expertise and sound engineering judgment and knowledge of product reliability principles. FMEA Analysis also requires a systems engineering approach to generate the retention rationale. It is also an important tool in the overall design process and risk management process.

Chapter 3: Hazard Analysis

WHAT IS HAZARD ANALYSIS?

MIL-STD-882D Standard Practice for System Safety defines a Hazard as "any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment" and a Hazardous Material as "any substance that, due to its chemical, physical, or biological nature, causes safety, public health, or environmental concerns that would require an elevated level of effort to manage."[8] Hazard Analysis starts with identifying the conditions or materials that exist that have the potential to cause harm resulting in a mishap and then working to determine how to control the hazards or materials. It is important to note that hazards or hazardous materials do not always result in mishaps. Proper controls are put in place to ensure that undesired events do not occur in the presence of hazards or hazardous materials.

Figure 2 depicts how Hazard Analysis should precede an approved design. As the Hazard Analysis is completed, it will show how to bring the risk down to a level accepted by the program or project and then the design team can incorporate the required features in the final design.

[8] Department of Defense. *MIL-STD-882D Standard Practice for System Safety.* Washington: Department of Defense. 2000. 1 – 2. Web 4 November 2010.

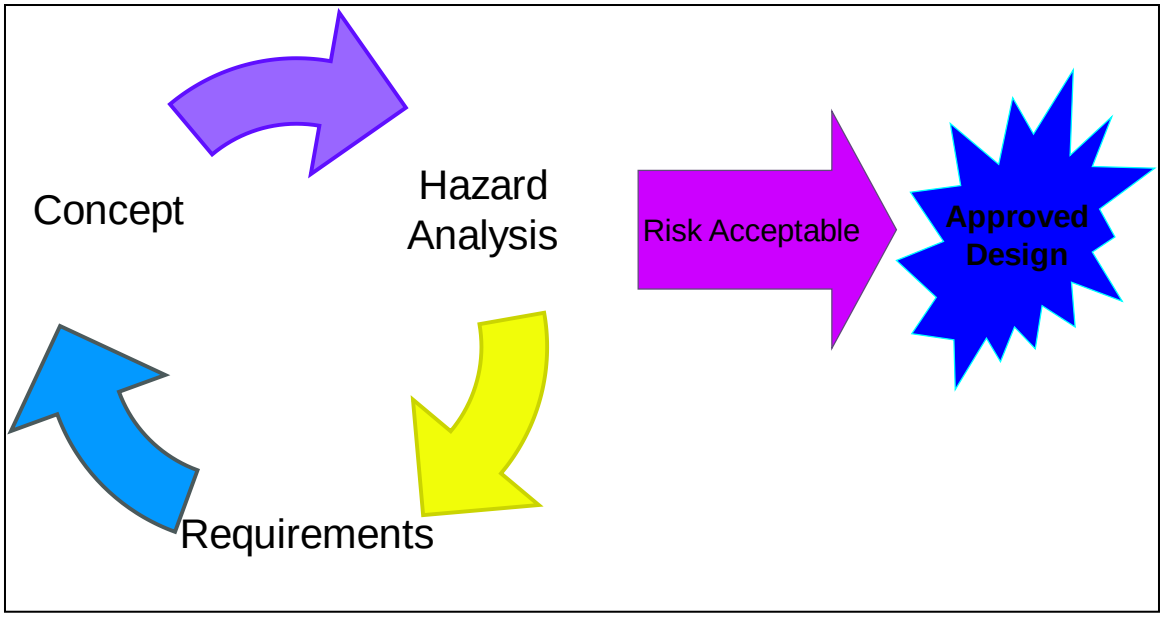

Figure 2 – Hazard Analysis in the Systems Engineering Process

Hazard Analysis is a top down structured intellectual process to review a system looking for conditions that if left unmitigated will result in a harmful effect and to identify features to mitigate those conditions.

HISTORY OF HAZARD ANALYSIS AT NASA

The initial reliability and quality assurance requirements for the Apollo program did not include any discussion of Hazard Analysis.[9] Hazard Analysis was not a key part of manned spaceflight until after the Apollo 1 fire on the pad.[10] Prior to that incident, the only "flight safety" that was considered was closely related to what the Occupational Safety and Health Administration evaluates

---

[9] Levine, Joe, Marion Merrell and Jeff Adams. *JSC SR&QA Evolution Resulting from Manned Spacecraft Program History.* Working Paper. 2002. 6. Print.

[10] Deans, Phil. "RE: Another HA Question." Message to Lisa Moore. 18 October 2010. E-Mail.

today, e.g. facility safety, slips, trips, and falls.[11] After the Apollo 1 fire on the launch pad, Boeing was tasked to perform independent analyses to review the overall safety, reliability and hazard assessments. This was the beginning of Hazardous Operations Analyses at NASA pushed primarily by the accident investigation and reconstruction boards and panels. NASA wanted to learn from their mistakes and install more pre-analyses and rigor in their design, development and operational systems. This effort resulted in more extensive Safety Analyses Reports and Critical Process Reviews and the identification of the controls and mitigation techniques that were added to program documentation.[12]

OBSTACLES IN THE HAZARD ANALYSIS PROCESS

Sometimes programs or projects get overwhelmed by the Hazard Analysis process because it breaks down and can easily become time consuming by letting the task of producing the Hazard Report become the goal rather than doing the analysis and updating the system design or implementing controls to increase safety. The Hazard Analysis process needs to start early in the life cycle, as early as the conceptual phase, with proper management support to gain the full benefit of the analysis. Like FMEA Analysis there can be obstacles in the process:

- Not starting the process in the early conceptual phase of the project
- Not fully understanding the system design and operation
- Skipping ahead in the process and jumping to a design solution.

---

[11] Levine, Joe. Personal Interview. 19 November 2008.

[12] Deans, Phil. “RE: Another HA Question.” Message to Lisa Moore. 18 October 2010. E-Mail.

THE ANALYSIS PROCESS

Define Your System of Interest

Before you can begin your analysis you need to know what your system of interest is and how it works. Consider all of the elements listed below and ensure that the entire team has a common understanding.

- Description – use block diagrams and other models.
- Boundaries – where the system begins and ends is very important as you consider the effects of the failures.
- Interfaces – you need to know all of your interfaces to ensure that you understand how failures in your system could affect other systems.
- Functions – how your system works and what it is supposed to do.
- Ground Rules and Assumptions – document any assumptions and ground rules that the team has agreed to.

Identify Hazardous Conditions

This should be a brainstorming exercise of discovery with your team members relying heavily on your engineering training and experience along with the knowledge of the operation of your system. Ask the question “What is inherently dangerous about the operation of your system?” Use generic hazard lists, hazard reports from heritage or legacy systems, lessons learned, and failure histories. You need to be sure to consider hazards that you could cause on interfacing systems and hazards from them that could impact your system. This step is where people often confuse hazardous conditions with the hazardous state. Hazardous conditions alone do not result in mishaps or catastrophic events; it takes an initiating event to turn a hazardous condition into a bad day. Table 1 shows examples of hazards, possible initiating events and potential undesired events.

Table 1 – Examples of Hazardous Conditions

Hazardous Condition	Initiating Event	Undesired Event
Flammable Liquids	Ignition Source e.g. spark	Explosion
Hot Surface	Human error	Burn
Pressurized Container	Rupture	Explosion
Lasers	Pointing error	Blindness
High Voltage	Human error	Shock
Two Spacecraft in Proximity Operations	Failure in attitude control system	Collision
RF Transmission	Pointing error	Exposure to radiation
Radioactive Materials	Compromise of storage container	Exposure to radiation

Identify the Effect of the Hazardous State

Given the hazardous condition, postulate all of the undesired events that could happen given the potential to cause harm of the hazard. Identify unplanned events that could result in death, injury, occupational illness, damage to or loss of equipment or property or damage to the environment. At this point in the analysis do not consider or eliminate effects based on presumed likelihood of occurrence, all credible effects must be evaluated.

Identify the Severity of the Effect

Once the effects are identified, using guidelines established by the project categorize the severity of the effects of the mishap. The standard categories from *MIL-STD-882D Standard Practice for System Safety* are:

- Catastrophic – Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation.

- Critical – Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200K but less than $1M, or reversible environmental damage causing a violation of law or regulation.
- Marginal – Could result in injury or occupational illness resulting in one or more lost work day(s), loss exceeding $10K but less than $200K, or mitigatable environmental damage without violation of law or regulation where restoration activities can be accomplished.
- Negligible – Could result in injury or illness not resulting in a lost work day, loss exceeding $2K but less than $10K, or minimal environmental damage not violating law or regulation.[13]

Identify all Potential Causes of the Hazardous States

This step can rely on many different analysis techniques including FMEA Analysis or Fault Tree Analysis to identify all of the possible initiating events that can turn a hazardous condition into a mishap or catastrophic failure. The analysis team needs to identify all unsafe acts or conditions that could lead to the hazardous event. The causes need to be indentified down to the level of the system at which the controls are to be applied. When looking for causes, the team should consider environmental conditions, hardware failures, software errors, procedural errors, personnel action or inaction, and component interactions (e.g. sneak circuits).

---

[13] Department of Defense. *MIL-STD-882D Standard Practice for System Safety.* Washington: Department of Defense. 2000. 18. Web 4 November 2010.

Identify Controls for each of the Hazard Causes

The dream of any program or project manager would be to field a hazard free system. Given the nature of most complex systems, it would be impossible or impractical to achieve this goal. There is residual risk with any space system; to minimize this risk the hazard causes must be controlled. Regardless of the program that you are working in, there is an accepted order of precedence to reduce the risk of the operation of the system. The first line of defense should always be changing the design to eliminate or minimize the effects of the hazardous condition. The system safety design order of precedence is:

- Eliminate hazards through design selection. If unable to eliminate an identified hazard, reduce the associated mishap risk to an acceptable level through design selection.
- Incorporate safety devices. If unable to eliminate the hazard through design selection, reduce the mishap to an acceptable leve using protective safety features or devices.
- Provide warning devices. If safety devices do not adequately lower the mishap risk of the hazard, include a detection and warning system to alert personnel to the particular hazard.
- Develop procedures and training. Where it is impractical to eliminate hazards through design selection or to reduce the associated risk to an acceptable level with safety and warning devices, incorporate special procedures and training. Procedures may include the use of personal protective equipment. For hazards assigned Catastrophic or Critical mishap severity categories, avoid

using warning, caution, or other written advisory as the only risk reduction method.[14]

Identify the Likelihood of Each Cause

For this step in the analysis process, the team should assume that the controls have been implemented. Now evaluate the likelihood that the undesired event will occur. This is a qualitative assessment performed to determine the likelihood of the worst case effects of the hazard being manifested. The team should consider the following when determining the likelihood: previous failure history, heritage systems, reliability assessments, strength of the controls. Again, each program or project may define their own likelihood categories. The standard categories from *MIL-STD-882D Standard Practice for System Safety* are:

- Frequent – Likely to occur often in the life of an item with a probability of occurrence greater than 10^{-1} in that life.
- Probable – Will occur several times in the life of an item with the probability of occurrence of less than 10^{-1} but greater than 10^{-2} in that life.
- Occasional – Likely to occur sometime in the life of an item with the probability of occurrence of less than 10^{-2} but greater than 10^{-3} in that life.

---

[14] Department of Defense. *MIL-STD-882D Standard Practice for System Safety.* Washington: Department of Defense. 2000. 4. Web 4 November 2010.

- Remote – Unlikely but possible to occur in the life of an item with the probability of occurrence of less than 10^{-3} but greater than 10^{-6} in that life.
- Improbable – So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence of less than 10^{-6} in that life.[15]

Indentify Verification Strategies for the Controls

The verification strategies define how you will know that the controls are in place and are identical to the standard requirements verification methods that systems engineers are familiar with: test, analysis, demonstration and inspection. Once strategies are identified, a closed loop tracking system is used to track the verification to completion.

Track Verification to Closure

Hazard Analysis is an iterative process and should continue through system delivery. As the defined controls are identified they should be provided to the requirements team and the design team depending on the life cycle phase. As the requirements and the design change you may need to revisit the hazard analysis.

Generate Reports

This is the final step in the process and the format of the reports can be as simple as a spreadsheet documenting the analysis results to the volumes of

---

[15] Department of Defense. *MIL-STD-882D Standard Practice for System Safety.* Washington: Department of Defense. 2000. 19. Web 4 November 2010.

information captured for manned space programs. Each program or project will set the requirements for the documentation required. It should be noted that the Hazard reports should be updated as new information is realized during the design process. Typical elements of Hazard reports are:

- Scope of analysis – what's in and what's out – the system definition;
- System description – to the level required for management to understand your results;
- Hazard, effects, severity, causes, controls, likelihood, verification strategy;
- Supporting data – "In God we trust, all others bring data";
- Executive summary – the bottom line for management – what's critical and why it is acceptable to fly with the potential failure modes?

The reports are very important first they serve as documentation for management of the residual risk for the program or project and second they are an important historical reference for knowledge capture for programs with long lifetimes or for future programs wanting to take advantage of successful designs.

BENEFITS OF HAZARD ANALYSIS

Hazard analysis results in the identification of risks and the means of controlling or eliminating them. Hazard analysis also quantifies the risk for the Program/Project Manager. Properly incorporated in the design and development of a system the results of Hazard Analysis will ensure that the system is safer. Hazard Analysis results in the identification of risks and the means of controlling or eliminating them.

Chapter 4: Compare/Contrast FMEA Analysis and Hazard Analysis

So far, this paper has discussed the FMEA Analysis and Hazard Analysis processes. There are similarities in the processes; however there are important differences in the benefits.

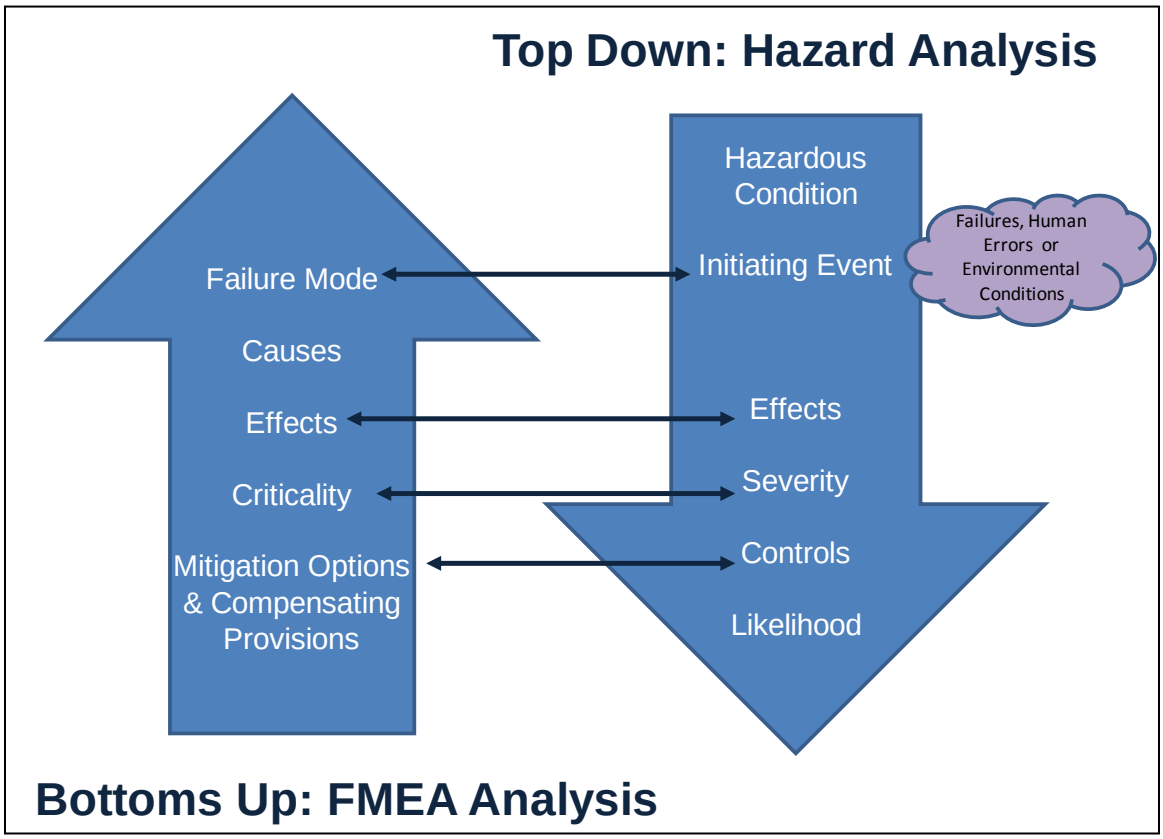

Figure 3 – Comparison of FMEA Analysis and Hazard Analysis

SIMILARITIES

Figure 3 shows **similarities** of the outputs for FMEA Analysis and Hazard Analysis.

- Failure modes may show up as initiating events in Hazard Analysis when FMEA Analysis is used to identify causes of mishaps.
- Effects for both techniques describe the undesired event.
- Criticality in FMEA Analysis is like the severity defined in Hazard analysis. Both attributes classify the failure mode or hazard by the criticality or severity of the effects. These classifications allow the project team to concentrate the most resources on the most critical or most severe items.
- Mitigating Options/Compensating Provisions for FMEA Analysis look much like the Controls from Hazard Analysis. Both items show the project how the engineering team has taken action to reduce the likelihood of the undesired effect from occurring or defined actions that can be taken to lessen the severity of the effects if the failure occurs or the hazardous condition is initiated.

DIFFERENCES

Although there are similarities, there ARE major **differences**.

- Failure modes of a system that are identified in FMEA Analysis will not encompass all of the initiating events identified by Hazard Analysis that could trigger an undesired event. And conversely the initiating events identified by Hazard Analysis will not identify all of the failure modes postulated during FMEA Analysis.
- FMEA Analysis is a bottoms up analytical process that starts at the component or subassembly level of a system, postulates all of the ways that the component or subassembly could fail and then identifies the effects of those failures. Hazard Analysis is a top down process that starts with the question “what is inherently

dangerous about my system?" and then seeks to identify all of the initiating events that could trigger mishaps. For example, when performing Hazard Analysis on an auxiliary power unit (APU) the analysis team would consider the hazardous condition of the pressurized volume and an initiating event of a rupture resulting in an explosion. They would put appropriate controls in place to minimize the risk of the explosion. The Hazard Analysis would not consider hardware failures resulting in loss of function of the APU, whereas FMEA Analysis would. If the analysis team only considers hazardous events such as explosion, they would miss failure modes such as failed closed valves resulting in loss of the APU function.

- FMEA Analysis does not consider human error in the analysis it only considers how the system can fail whereas Hazard Analysis considers human error, failures, and environmental conditions as initiating events for the mishaps.
- Hazard Analysis controls typically include things like fault tolerance, factors of safety, and operational workarounds to minimize the effects of the undesired condition. FMEA Analysis delves deeper into material compatibility, parts selection, specific screening tests and inspections to control the failure mode causes.

The implementation of the results of FMEA Analysis will ensure that the system will perform reliably and the implementation of the results of Hazard Analysis will ensure the system will operate safely.

Chapter 5: Myths about FMEA Analysis and Hazard Analysis

There are many myths about FMEA Analysis and Hazard Analysis. Most of the confusion is due to lack of understanding of the process and benefits of the products of the two analysis techniques.

MYTH #1: FMEA AND HAZARD ANALYSIS REPORTS ARE NOT USED OVER THE LIFE OF THE PROJECT

Some systems engineers in the unmanned world of NASA have the idea FMEA Analysis and Hazard Analysis are not useful after the early milestones in the project life cycle. Some even see the products from the two analysis techniques simply as deliverables listed on the contract data requirements list and once they are delivered they have "checked the box" and can move on to the other parts of the system design. This thinking is erroneous and short sighted and leads to missed opportunities in the areas of cost savings, reduced efficiency, and schedule risk of finding disconnects later in the life cycle. That is unfortunate since there is so much valuable information that can be gleaned from the results of the two analysis techniques. When done properly, the system can benefit via improved requirements, design, tests, inspections, and special procedure or workarounds. The resulting reports should be put under configuration management and tracked to ensure that the improvements are carried out in the final design, verification and use of the system.

Using FMEA Analysis Results

The mitigation options and compensating provisions from FMEA Analysis should be used as follows:

- Design – there should be ample opportunity to influence the design to either eliminate the cause of the failure mode or to reduce the likelihood that the failure will occur due to the causes identified. The design features identified in the FMEA Reports need to be tracked through the design review milestones to ensure that the recommended design changes were implemented.
- Test – during the analysis specific tests were identified to detect the presence of the specific causes and failure modes identified. As the verification methods are developed, there needs to be assurance that these tests have been incorporated in the acceptance of the system prior to first use to ensure that the failure cause doesn't exist. These tests can be part of the design qualification tests, tests during the assembly and integration process, or they could be final tests prior to first use.
- Inspection – The same thing applies for inspection as for tests. If the analysis identified ways to inspect for the failure cause, there needs to be assurance that these inspections made their way into the manufacturing process.
- Mitigating Options and Compensating Provisions – The special operational techniques that were identified in the analysis process need to be added to flight rules, operating procedures, or special training to ensure that if the failure does occur, the process is in place to circumvent or mitigate the effects of the failure.

Using Hazard Analysis Results

The controls from the Hazard Analysis should be used as follows:

- Design – the results of the hazard analysis can also influence the design and should be tracked through the design reviews.

- Safety Devices – there needs to be verification that any safety devices that were identified in the analysis process have been implemented in the design and should be tracked through the design reviews.
- Caution and Warning – there needs to be verification that any caution and warning devices such as warning lights or claxons that were identified in the analysis process have been implemented in the design and should be tracked through the design reviews. In addition to hardware caution and warning; warnings and cautionary notes, labels or marking should be provided for assembly, operation and maintenance activities.
- Special Procedures – there needs to be verification that any special procedures that were identified in the analysis process have been implemented in the appropriate assembly, operation and maintenance procedures.

The bottom line is that all of the results from the two analysis techniques need to be incorporated in the overall systems engineering process over the entire life cycle to ensure that the final system is both safe and reliable.

MYTH #2: YOU DON'T NEED TO DO BOTH FMEA AND HAZARD ANALYSIS

As discussed in Chapter 4, the similarities between FMEA Analysis and Hazard Analysis have led some to say that you get everything you need with only one of the analysis techniques and perhaps they could save project resources by eliminating the requirement to perform one of the processes. There is also confusion since FMEA Analysis is sometimes used in Hazard Analysis to help identify initiating events that result in mishaps. The FMEA Analysis done in direct support of Hazard Analysis is only looking at failure modes that would serve as initiating events for that particular hazardous condition and should not be

considered the all inclusive analysis for a particular system. If FMEA Analysis is eliminated, Hazard Analysis will result in a classification of how critical the undesired event is, you get a likelihood of the undesired event occurring and you get a list of methods to control or deal with the undesired event. However, you may miss critical failure modes or critical hazards if both analyses are not performed. Consider the following examples:

FMEA Analysis Will Miss a Critical Hazard

The Ku-Band Radar and Communications System onboard the Space Shuttle Orbiter consists of three avionics boxes and an antenna assembly (called the Deployed Assembly) mounted in the payload bay shown in Figure 4. The Deployed Assembly has gimbal motors that by the nature of their design are not explosion proof, in other words they can act as an ignition source in a volatile environment.

Figure 4 – The Ku-Band Deployed Assembly on the Space Shuttle Discovery inside the Orbiter Processing Facility Bay 3 at NASA's Kennedy Space Center, Credit: NASA.

FMEA Analysis was performed to identify the ways that the motors could fail and there are FMEA reports documenting failure modes result in losing the function of the gimbal motors and how that impacts the performance of the Ku-

Band System and on the overall Shuttle mission. However, the FMEA Analysis does not address what would happen if the system was operated in a volatile environment. That situation was addressed when the engineering team asked the question, “What is inherently dangerous about the operation of the system?” The gimbal motors were identified as the hazard. There are operations as the Orbiter is being processed at the Kennedy Space Center where volatile gases could be present. That would be the initiating event and the worst case effect would be an explosion if the Ku-Band System was operated in that environment. So controls were put in place for operations with the Orbiter that doesn’t allow the Ku-Band to be operated when there are volatile gases present in the facility and vice versa. To date there have been no incidents of explosions in the processing facility related to the Ku-Band System gimbal motors. Without the Hazard Analysis, this hazard may have been overlooked until a mishap occurred.

Hazard Analysis Will Not Identify All Failure Modes

Since Hazard Analysis asked what is dangerous about operating a system, it has the potential to overlook failure modes that do not manifest as mishaps. Yet, the effects of these other failure modes are very important for mission success. Again looking at the Ku-Band Radar and Communication System on the Space Shuttle Orbiter, the Ku-Band System provides a critical service to the overall success of a Space Shuttle mission. It provides downlink of high rate data from payloads on the Orbiter and downlink of live television. The Ku-Band System is a complicated system with many electrical and mechanical parts with many potential failure modes any one of which could result in the loss of the high rate downlink function. Loss of this function is not inherently dangerous to the Space Shuttle mission so many of these failure modes would not be addressed with the proper controls through Hazard Analysis. Without FMEA Analysis to identify the many failure modes and address the causes

through improvements in design, test and inspection; the reliability of the Ku-Band System would be much less than it is today.

MYTH #4: FMEA ANALYSIS WON'T TELL ME ANYTHING THAT I DON'T ALREADY KNOW

Some design engineers feel that they know more about their system than their reliability counterparts. While that may be true, there is opportunity to improve system designs when all of the possible failure mechanisms that may cause the system to fail. The design engineers may not be aware of all of the options available to improve the reliability of their design such as parts selection, Some systems engineers feel that they know where all of the single point failures that would kill their mission so, they do not need to do FMEA Analysis. If a system has single failure points, there is a stronger need to perform the analysis to identify design solutions to eliminate or mitigate failure mode causes to control. Either way, to ensure the most reliable system design, a multi-disciplined team is required to ensure that all likely failure modes and their probable effects are identified and dealt with properly.

MYTH #5: FMEA ANALYSIS WON'T DISCOVER EFFECTS ON THE END ITEM

The Goddard Spaceflight Center is currently developing the four spacecraft for the Magnetospheric Multiscale (MMS) mission. The MMS mission is a Solar-Terrestrial Probe mission comprising four identically instrumented spacecraft that will use the Earth's magnetosphere as a laboratory to study magnetic reconnection. As shown in Figure **5**, there are four 58 meter wire booms to measure electrical fields attached to each of the four spacecraft. As with most spacecraft there is a propulsion system responsible for providing an orbital maneuvering capability.

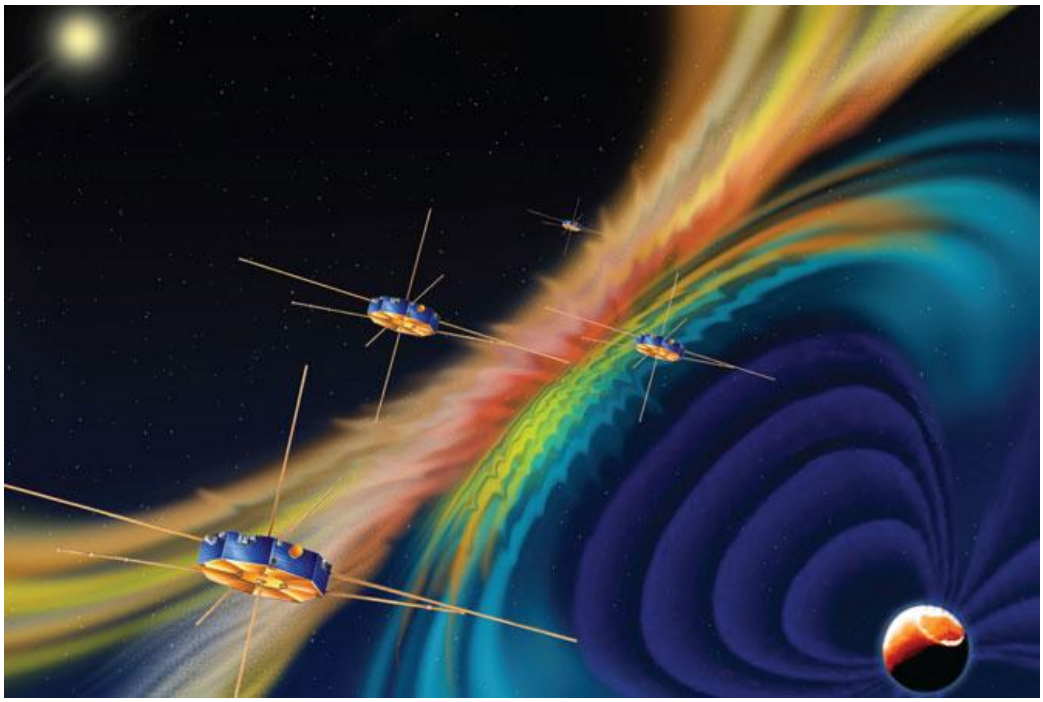

Figure 5 – Artist conception of the four MMS spacecraft. Credit: Southwest Research Institute.[16]

Consider the FMEA Analysis that would be performed on a thruster in the propulsion system on the spacecraft. It was surmised that the engineer performing the FMEA Analysis on the thruster would not know all the effects of a failure of the thruster would be on the spacecraft and its overall mission, including that exciting the wire booms such that they could be wrapped around the spacecraft or other rigid booms. This is where it is important to note the FMEA Analysis should not be an individual sport. It should be a team sport with the correct skill mix and systems knowledge to ask the right questions. For example, back to the potential failure of a thruster on one of the MMS spacecraft.

---

[16] Hendrix, Susan. "NASA's Magnetospheric Mission Passes Major Milestone." *The Latest from Heliophysics*. NASA/Goddard Spaceflight Center, n.d. Web. 02 Nov 2010. <http://www.nasa.gov/topics/solarsystem/sunearthsystem/main/mms-cdr.html>.

One of the failure modes of a thruster is that it inadvertently provides thrust. Following the FMEA Analysis process discussed in Chapter 2, look at effects at all levels up to and including effects on the spacecraft. Consider the following questions that the analysis should address when determining the effects of an inadvertent thruster firing:

- What happens to the spacecraft? The spacecraft could be sent off course or start to rotate in an undesirable state.
- What happens to all of the booms attached to the spacecraft if it begins to rotate in an undesirable state? The physical characteristics of each of the booms and their relationship to each other would have to be evaluated by a team of experts to determine if any undesired interactions between the booms would occur due to the unplanned motion of the spacecraft.

If the team of engineers followed the prescribed FMEA Analysis methodology and asked the right questions and considered the effects on the whole spacecraft, these critical effects will be identified early in the design process and assurances put in place to ensure proper operation of the thrusters to minimize the likelihood of compromising a mission due to a failed thruster. When executed properly FMEA Analysis will identify effects of failed components or subassemblies on the overall system.

Chapter 6: Benefits to Program Management

The goal of every program or project manager is to have a safe reliable product and to have an understanding of the residual risk of operating that product. In order to accomplish that goal the manager relies on his systems engineering team to design the best system to meet the mission objectives. FMEA Analysis and Hazard Analysis are two of the very important tools that can be used to meet that goal.

The greatest criticism of FMEA Analysis has been its limited use in improving system designs. The chief causes for this are that the FMEA Analysis is not performed early enough in the design process and the performance of the analysis has been isolated from the design process.[17] If the Reliability engineers worked together with the design and systems engineers then the FMEA Analysis would be more comprehensive and value added changes to the design could be made early in the design process. Therefore, FMEA Analysis should be initiated as soon as preliminary design information is available at the higher system levels and extended to the lower levels as more information becomes available on the items in question.

FMEA Analysis results in the identification of critical items and their associated retention rationale for decision making purposes. FMEA Analysis will define design options to eliminate the failure cause, improve system reliability to minimize failure likelihood, or reduce the severity of the effect if the failure does occur. It will also define methods for fault detection and recovery including

---

[17] Department of Defense. *MIL-STD-1629A Procedures for Performing a Failure Mode and Effects and Criticality Analysis.* Washington: Department of Defense. 1980. iii. Web 4 November 2010.

inspection points, tests, telemetry, or operational workarounds. The results of FMEA Analysis can be used by quality assurance in the planning and control of critical processes to ensure a reliable system. Of most value to the program or project manager is the identification of critical items for use in their risk management.

The results of FMEA Analysis should be considered for all life cycle phases of a system. Although one of the most visible places where the FMEA Analysis results are used is system design; the results can also be used to improve maintainability, identify initiating events in Hazard Analysis, logistics support, maintenance plans, and for failure detection and fault isolation. FMEA Analysis results can be used to improve tests to verify performance in all operating conditions. For example, the FMEA Analysis for a particular infrared Earth sensor indicated the existence of a failure mechanism at the upper operating temperature which would only be detectable if the infrared sensor was stimulated by an infrared source at that temperature. Unfortunately the FMEA was not used during the preparation of the test procedure, the sensor was not stimulated during thermal testing and a fault occurred in orbit. A $100 million project was thus unnecessarily jeopardized.[18]

Hazard Analysis provides assurance to the project that the design is safe as possible, that the requirements address hazard mitigation and that the risk is properly identified. Hazard Analysis is used as a design tool influencing the design to reduce if not eliminate hazardous conditions. The results of the Hazard Analysis can also be used to assist in validation of the system requirements. Incorporating the controls into the system requirements will help to ensure that

---

[18] Fortescue, Peter W., John Stark, and Graham Swinerd. *Spacecraft Systems Engineering*. New York: J. Wiley, 2003. 556. Print.

the requirements are complete ensuring that the project will “build the right thing”. After all of the Hazard Analysis is complete, the main value to the project will be as a risk assessment and risk management tool. While in some cases safety risk can be eliminated, in most cases a certain degree of safety risk must be accepted. In order to quantify expected accident costs before the fact, the potential consequences of an accident, and the probability of occurrence must be considered. The summary of the hazard analysis results in an overall relative risk ranking for the project/program to identify where the greatest resources should be applied toward risk reduction. The safest thing to do is to never fly; in order to fly you must accept a certain level of risk. The results of the Hazard Analysis quantify that risk so that it can be managed.

The results of FMEA Analysis and Hazard Analysis are also important in the overall risk management of a program or project. Once the criticality of the failure modes and the severity of the hazards have been identified, the program or project manager can concentrate their resources on the most critical and most severe items; thus focusing their efforts to get the best return on their resource investment in the area of risk management.

Chapter 7: Integrating Analysis Results into the Systems Engineering Process

As discussed before, books and reference materials on Systems Engineering do discuss safety and reliability usually as a specialty engineering discipline to supplement the overall systems engineering process. It should be noted that in order to get the best system possible, safety and reliability need to be integrated into the whole process from the conceptual stages of a project through operations and disposal. The consideration of failure potential, or mission risk, of a system is an essential part of systems engineering. In order to ensure that a reliable and safe system is designed, it is important to understand the failures that will impact mission success and the hazards that will result in mishaps and take appropriate actions to eliminate or mitigate the causes.

FMEA Analysis and Hazard Analysis must be part of the overall systems engineering process over the entire life cycle of the project and should not be considered tasks that are completed to “check the box” to meet a contract deliverable and put the reports on a shelf. The results of both analyses need to be used as discussed to improve the overall mission success and safety of the system. There are two “sides” to integrating these processes into the systems engineering process. First is the technical side and how the processes fit into the system life cycle. Second is the overcoming the obstacles to and myths surrounding the FMEA and Hazard Analysis processes.

Integrating FMEA and Hazard Analyses into the Systems Engineering Process

Table 2 shows where FMEA and Hazard Analysis fit into the overall system life cycle and how the results are used to improve the safety and reliability of the system.

Table 2 – FMEA Analysis and Hazard Analysis throughout the System Life Cycle

Pre-Phase A & Phase A Conceptual Development	Phase B Preliminary Design	Phase C Final Design and Fabrication	Phase D Assembly, Integration, Test & Launch	Phase E Operations
Preliminary Hazard Analysis identifies high level hazards and provides initial input to design team for control strategy.	• Influence design through definition of control strategy and specific controls as the design matures. • Define control verification strategy.	• Finalize verifications. • Track verifications to ensure controls are incorporated in the design	• Track verifications to closure to ensure controls are in place and function as intended to reduce risk. • Use operational controls as basis for operator training.	• Use operational controls as required if failures occur. • Use Hazard Analysis to assess changes in risk associated with proposed design and/or operational changes.
	FMEA Analysis to influence design	Ensure that FMEA Mitigation Options were incorporated in Design	Ensure that FMEA Mitigation Options are incorporated in Assembly, Integration &Test	Use FMEA Compensating Provisions as required if failures occur.

During the conceptual development phase of the project, hazard analysis identifies inherently hazardous design and operational characteristics. Thought is also given to the preliminary severity of the potential hazards to ensure that proper safety requirements are documented in the System Requirements Document. Preliminary FMEA Analysis is started to evaluate the functional criticality of the system to ensure that the proper fault tolerance requirements are levied in the system requirements document.

As the system design matures to the preliminary design phase, Hazard Analysis can start identifying additional initiating events through fault tree and other related analysis techniques progress. The FMEA Analysis can start as the detailed design has started. Results of the FMEA Analysis should begin to influence the design using product reliability best practices.

As the system passes the final design phase and begins fabrication, both the FMEA and Hazard Analysis should be complete and the results used to validate the design in accordance with the mitigation options and controls defined in the analysis processes. Inspection and Test Retention Rationale from the FMEA Analysis should be integrated into the assembly, integration and test phase of the system development to ensure that failure mode causes do not exist in the final system.

During the operational phase of a system, compensating provisions identified in the FMEA and Hazard Analyses can be used to negate or mitigate the effect of a failure.

Overcoming the Obstacles and Myths

As discussed in chapters 2 and 3, there are obstacles in performing the two analysis techniques. There are also myths to overcome to reset the paradigm of design engineers and systems engineers as discussed in chapter 5. Most of these obstacles and myths can be overcome with training on how to perform the analysis process and a greater understanding of how the results can improve a program or project. Training the entire team on the methodologies for FMEA Analysis and Hazard Analysis will improve the overall understanding and value of the results of the processes. Program and Project Managers need to be trained as well; this will ensure that they understand the return on their investment in allocating resources to perform FMEA Analysis and Hazard Analysis at the appropriate times in the life cycle. Although not the main focus of this paper, the need for an overall paradigm shift of how reliability and safety engineers are integrated into overall systems engineering team is required. That shift requires a change in the way the reliability and safety engineers participate in the systems engineering activities. The reliability and safety engineers need to:

- Have a firm understanding of the FMEA Analysis and Hazard Analysis processes. This includes not just being a "process policeman" for the two analysis processes; it includes understanding how the processes work and how to apply them to their project.
- Understand the system that they are working with.
- Become a GREAT reliability and/or safety engineer:
  - A GOOD reliability/safety engineer can identify what can go wrong.
  - A BETTER reliability/safety engineer can identify what can go wrong and determine how likely it is.
  - A GREAT reliability/safety engineer can identify what can go wrong, determine how likely it is AND tell you how to avoid it.[19]

It really comes down to the old adage that you should bring solutions not just problems to your manager. Anyone can be a critic; a GREAT reliability/safety engineer brings solutions.

With improved training and a paradigm shift, FMEA Analysis and Hazard Analysis can be properly integrated into the systems engineering process and result in increased reliability and safety for programs and projects.

---

[19] Frost, John. *System Safety Engineering: The Rodney Dangerfield of the Design Team?* Print.

Chapter 8: Summary

All projects can benefit from FMEA Analysis and Hazard Analysis. The results of the two analysis techniques will improve system requirements, system design, overall system reliability and safety. The project will have a better understanding of their overall risk and how to manage it. Since design changes can be implemented earlier in the project life cycle and the overall mission success rate will be improved, this can translate into overall cost and schedule savings.

FMEA Analysis is a structured intellectual process to identify all credible failure modes, eliminate failure modes by design if possible, manage the remaining failure modes and their causes, and quantify the risk based on the criticality of the effects of the failure modes. FMEA Analysis is not an exact science, it relies on engineering expertise and engineering judgment, relies on knowledge of product reliability principle and requires a systems engineering approach to identify the mitigation options and compensating provisions. FMEA Analysis is an important tool in the overall design process and risk management for a system. 24.8% of the documented spacecraft failures from 1962 – 1988 were caused by poor design.[20] Incorporating a rigorous FMEA Analysis process will ensure that system reliability was “designed in”.

Hazard Analysis is a structured intellectual process to identify risk, classify risk and manage risk. Hazard Analysis is not an exact science it also relies on engineering expertise and engineering judgment. Hazard Analysis is an important tool in the design process, requirements validation and risk management.

---

[20] Larson, Wiley J., and James R. Wertz (editors). Space Mission Analysis and Design. Torrance, CA: Micrcosm, Inc. 1992. 709. Print.

The purpose of this report was to show the value in both FMEA and Hazard Analysis. The value can only be added to a program or project if management is willing to take the additional time at the beginning of a program or project to properly integrate the processes into the systems engineering process and carry them throughout the project life cycle. This includes committing resources to properly training the project staff on these two analysis techniques and allowing time for the analysis to be completed to improve overall system reliability and safety.

References

Blanchard, Benjamin S. *Systems Engineering Management*. 2nd ed. New York: Wiley, 1998. Print.

Deans, Phil. “RE: Another HA Question.” Message to Lisa Moore. 18 Oct. 2010. E-mail.

Department of Defense. *MIL-STD-882D Standard Practice for System Safety*. Washington, DC: Department of Defense, 1980. *Google Search*. Web. 4 Nov. 2010. <http://www.acq.osd.mil/atptf/policy/documents/MILSTD882D.pdf>.

Department of Defense. *MIL-STD-1629A Procedures for Performing a Failure Mode and Effects and Criticality Analysis*. Washington, DC: Department of Defense, 2000. *Google Search*. Web. 4 Nov. 2010. <http://sre.org/pubs/Mil-Std-1629A.pdf>.

Ericson, Clifton A. *Hazard Analysis Techniques for System Safety.* Hoboken, New Jersey: John Wiley & Sons, 2005. Print.

Fortescue, Peter W., John Stark, and Graham Swinerd. *Spacecraft Systems Engineering*. New York: J. Wiley, 2003. Print.

Frost, John. *System Safety Engineering: The Rodney Dangerfield of the Design Team?* Print.

Hendrix, Susan. "NASA's Magnetospheric Mission Passes Major Milestone." *The Latest From Heliophysics*. NASA/Goddard Spaceflight Center, n.d. Web. 02 Nov 2010. <http://www.nasa.gov/topics/solarsystem/sunearthsystem/main/mms-cdr.html>.

Larson, Wiley J. and James R. Wertz. *Space Mission Analysis and Design.* 2nd ed. Torrance, California: Microcosm, Inc., 1992. Print.

Levine, Joe. Personal interview. 19 Nov. 2008.

Levine, Joe, Marion Merrell and Jeff Adams. *JSC SR&QA Evolution Resulting from Manned Spacecraft Program History.* Working Paper. 2002. Print.

"Magnetospheric Multiscale Mission Concept." *STP Magnetospheric Multiscale Mission*. National Aeronautics and Space Administration, n.d. Web. 02 Nov 2010. <http://stp.gsfc.nasa.gov/missions/mms/mms.htm>.

"MMS Spacecraft." *Magnetospheric Multiscale Mission*. Southwest Research, n.d. Web. 02 Nov 2010. <http://mms.space.swri.edu/spacecraft.html>.

National Aeronautics and Space Administration. *NASA/SP-2007-6105 NASA Systems Engineering Handbook*. Washington, DC: National Aeronautics and Space Administration, 1995. Print.

O'Connor, Patrick D. T. *Practical Reliability Engineering.* 4th. West Sussex: Wiley, 2002. 2. Print.

Stamatis, D. H. *Failure Mode and Effect Analysis: FMEA from Theory to Execution*. 2nd ed. Milwaukee, Wisconsin: ASQ Quality Press, 2003. Print.

Vincoli, Jeffrey W. Basic Guide to System Safety. Hoboken, NJ: Wiley-Interscience, 2006. Print.

Vita

Alicia Louise Leonard Moore graduated from the University of Texas at Austin in 1986 with a Bachelors of Science in Electrical Engineering; she accepted her first technical job with the Boeing Aerospace Corporation in Houston, TX in 1986. She served as a Reliability Engineer assigned to the Tracking and Communications subsystems of the Space Shuttle Orbiter in support of the Safety, Reliability and Quality Assurance (SR&QA) contract for the Johnson Space Center (JSC). It was there she first learned to perform Failure Modes and Effects Analysis as part of the post-Challenger accident return to flight activities. She accepted a job with the National Aeronautics and Space Agency in 1988 as a project engineer for the Ku-Band Radar and Communications System. She quickly progressed to Subsystem Manager for the Ku-Band System but never forgot her SR&QA roots. After her tenure as Ku-Band Subsystem Manager, she served as a Mission Evaluation Room Manager for the Orbiter Project Office; then returned to the Engineering Directorate to serve as Project Manager for the Communication System Upgrade for the Space Shuttle Program; later served as Space Shuttle Independent Assurance Manager for the Human Exploration and Development of Space Independent Assessment Office; led the requirements development effort for the Orbital Space Plane Program as the Requirements Lead; prior to leaving the agency in 2005, was assigned to the JSC Office of the Chief Engineer. In 2006 she worked at Compliance Automation training NASA engineers across the agency as well as

other corporate clients in Requirements Definition and Management. In 2007 she returned to JSC to work for Science Applications International Corporation in support of the Safety and Mission Assurance contract. In 2010 she rejoined NASA at the Goddard Space Flight Center in Greenbelt, MD. She is currently is a systems engineer for the Landsat Data Continuity Mission and hopes to bring enthusiasm about the safety and reliability side of systems engineering to her colleagues at the Goddard Spaceflight Center.

Email: lisa.moore@nasa.gov

This report was typed by Alicia Louise Leonard Moore